AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with 12 SUBJECT FILES associated with SUBJECT CYBERTIPS stored on an encrypted thumb drive	)	Case No. MJ25-132

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Information associated with 12 SUBJECT FILES associated with SUBJECT CYBERTIPS stored on an encrypted thumb drive located in Bellingham, Washington

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)	Receipt or Distribution of Child Pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

✓ See Affidavit of FBI Special Agent Natalie Leavitt, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Natalie Leavitt
Applicant's signature

Natalie Leavitt, Special Agent
Printed name and title

◯ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 03/12/2025

Paula L McCandlis
Judge's signature

City and state: Seattle, Washington

Paula L. McCandlis, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Description of Property to be Searched

The following SUBJECT FILES associated with the SUBJECT CYBERTIPS, which are stored on an encrypted thumb drive currently located at the FBI office in Bellingham, Washington.

CYBERTIP Number: 133426894

- Associated with: IP Address 216.243.2.254
- ESP: Facebook
- SUBJECT FILE Name: bZmdXIol7RJo7vcJ10000000_4980617235398308_4515015360492102484_n.mp4
- SUBJECT FILE Type: B1

CYBERTIP Number: 187960570

- Associated with: IP Address 168.212.80.1
- ESP: Snapchat
- SUBJECT FILE Names:
  - talan.bungard-None-e43ee7a5-ab77-5ca8-be61-d22a5d5235a3~2227- 5f0d0bce99-content.jpg
  - talan.bungard-None-e43ee7a5-ab77-5ca8-be61-d22a5d5235a3~2238- f162da0b54-content.jpg
  - talan.bungard-None-AD7A0531-1C3F-4CF6-9492-AAFC403A62DD-4512511459-content.jpg
- SUBJECT FILE Types: B2

CYBERTIP Number: 182657806

- Associated with: IP Address 168.212.80.1
- ESP: Instagram

- SUBJECT FILE Name: kHdi3N8UsA7Dpnln411201837_338749462237448_2227901945770862706_n.mp4
- SUBJECT FILE Type: B2

CYBERTIP Number: 186170387

- Associated with: IP Address 4.37.69.186
- ESP: Google
- SUBJECT FILE Names:
  - PVK_5116.jpg
  - PVK_5886 (3).jpg
- SUBJECT FILE Types: Not specified

CYBERTIP Number: 183500836

- Associated with: IP Address 4.37.69.186
- ESP: Instagram
- SUBJECT FILE Name: z1RezETQgyRcK15B414981859_24346419101668041_8734993716765846851_n.mp4
- SUBJECT FILE Type: B1

CYBERTIP Number: 204173525

- Associated with: username sin_mied00
- ESP: Instagram
- SUBJECT FILE Name: OKF9zj5UNVO9V7Rt462577400_2030519530709476_8360420724942733043_n.jpg
- SUBJECT FILE Type: B1

CYBERTIP Number: 131334754

- Associated with: username jarvidylanr
- ESP: Facebook

- SUBJECT FILE Name: CC6InoOZrrGI2syO288244391_5247343785358433_4475858483811337 00_n.mp4
- SUBJECT FILE Type: Not specified

CYBERTIP Number: 11885149

- Associated with: username bellako_13
- ESP: Facebook
- SUBJECT FILE Names:
  - root-request-tempfiles7dnhaa660fgo0o4k13285671_624825027684548_1765048 393_n .jpg
  - root-request-tempfilesac7vlsaw1nsogggk13285671_624825027684548_1765048 393_n .jpg
- SUBJECT FILE Types: Not specified

CYBERTIP Number: 11884993

- Associated with: username bellako_13
- ESP: Facebook
- SUBJECT FILE Name: root-request-tempfilesdtmp0n18lds0c0kw13282063_1750882848459101_2117239048_ n.jpg
- SUBJECT FILE Type: Not specified

CYBERTIP Number: 72033948

- Associated with: everildo.mendoza.7
- ESP: Facebook
- SUBJECT FILE Name: 53ply2dz2rggow8095725654_2742387202550209_497172242117384061 8_n.mp4

- SUBJECT FILE Type: Not specified

CYBERTIP Number: 64996692

- Associated with: everildo.mendoza.7
- ESP: Facebook
- SUBJECT FILE Name: 20rr7g5r2r5wk4sg86802617_2905973956131291_6258471936714425512_n.mp4
- SUBJECT FILE Type: Not specified

CYBERTIP Number: 68660570

- Associated with: danieljuniorsantos127
- ESP: Facebook
- SUBJECT FILE Name: n99o5xwj828800cs92508571_599521230641971_4501033466015514624_o.jpg
- SUBJECT FILE Type: Not specified

ATTACHMENT B

ITEMS TO BE SEIZED

All information that constitutes evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found in the SUBJECT FILE:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct;

2. Information about the SUBJECT FILES related to the timing or circumstances of their creation and transmission; in any format or media;

3. Information concerning the identify of any individuals depicted in the SUBJECT FILES; and

4. Information or data that, including direct messages, postings, photos, or other account content that identifies the user(s) of the accounts associated with the SUBJECT FILES.

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF WHATCOM)

I, Natalie Leavitt, being duly sworn on oath, depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since 2022. I am currently assigned to the Bellingham Resident Agency of the Seattle Division and the FBI's Northwestern Washington Safe Trails Task Force ("NWSTTF"). I have attended several training courses including but not limited to Human Trafficking Investigations in September of 2024 and Human Trafficking in Indian Country in April of 2023. My primary responsibilities as a Special Agent include investigations involving violent crimes and other federal crimes on the Indian reservations in Northwest Washington. My duties as a special agent also include the investigation of those engaged in the sexual exploitation of children, including the production, attempted production, distribution, and possession of child pornography. I have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256(8), in various forms of media, including media stored on digital media storage devices such as computers, iPhones, etc. I have participated in the execution of numerous search warrants which involved child exploitation and/or child pornography offenses.

2. I am submitting this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the SUBJECT FILES associated with the following CyberTipline Reports (hereinafter "the SUBJECT CYBERTIPS"), fully described in Attachment A, for the things specified in Attachment B to this Affidavit, for the reasons set forth below.

- 133426894 – Submitted by Facebook
  - One file sent through Facebook Messenger on 06/21/2022 UTC by "Baki Garcia" with a category of B1.
- 187960570 – Submitted by Snapchat
  - Three files sent through Snapchat on 02/21/2024 UTC by "talan.bungard" with a category of B2.
- 182657806 – Submitted by Instagram
  - One file sent through Instagram on 12/16/2023 UTC by "EricTH" with a category of B2.
- 186170387 – Submitted by Google
  - Six files sent through Google on 02/02/2024 UTC by "Alex The Lost Johnson" with a category of B2.
- 183500836 – Submitted by Facebook
  - One file sent through Facebook Messenger by "Jose Herrera" on 12/30/2023 UTC with a category of B1.
- 204173525 – Submitted by Instagram
  - One file sent through Instagram by "wegonbeok" on 12/28/2024 UTC with a category of B1.
- 131334754 – Submitted by Facebook
  - One file sent through Facebook Messenger by "Jarvidylan Ramirez" on 06/24/2022 UTC with an unknown category.
- 11885149 – Submitted by Facebook
  - Two files sent through Facebook Messenger by "Juan De Dios Cokita Ramirez" on 05/26/2016 UTC with an unknown category.
- 11884993 – Submitted by Facebook
  - One file sent through Facebook Messenger by "Chepe Pk" on 05/26/2016 UTC with an unknown category.

- 72033948 – Submitted by Facebook
  - One file sent through Facebook Messenger by "Sergio Gonzales Gonzales" on 05/09/2020 UTC with an unknown category.
- 64996692 – Submitted by Facebook
  - One file sent through Facebook Messenger by "Sergio Gonzales Gonzales" on 02/26/2020 UTC with an unknown category.
- 68660570 – Submitted by Facebook
  - One file sent through Facebook Messenger by "Danyel Junior Santos" on 04/09/2020 UTC with an unknown category.

3. The warrant would authorize a search of the SUBJECT FILES for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) (the TARGET OFFENSES).

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience and my discussions with other law enforcement agents who have experience in investigating cases involving child sexual exploitation.

5. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of the TARGET OFFENSES, will be found within the SUBJECT FILES and the SUBJECT CYBERTIPS.

BACKGROUND ON NCMEC AND CYBERTIPS

6. I know based on my training and experience, that Electronic Service Providers ("ESP") and/or Internet Service Providers ("ISP," collectively ISP) typically monitor their services utilized by subscribers. To prevent their communication networks from serving as conduits for illicit activity and pursuant to the terms of user agreements, ISPs routinely and systematically attempt to identify suspected depictions of minors engaged in sexually explicit conduct that may be sent through its facilities. Commonly, customer complaints alert them that an image or video file being transmitted through their facilities likely contains suspected depictions of minors engaged in sexually explicit conduct.

7. When an ISP receives such a complaint or other notice of suspected depictions of minors engaged in sexually explicit conduct, they may employ a "graphic review analyst" or an equivalent employee to open and look at the image or video file to form an opinion as to whether what is depicted likely meets the federal criminal definition of depictions of minors engaged in sexually explicit conduct found in 18 U.S.C. § 2256, which is defined as any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. If the employee concludes that the file contains what appears to be depictions of minors engaged in sexually explicit conduct, a hash value of the file can be generated by operation of a mathematical algorithm. A hash value is an alphanumeric sequence that is unique to a specific digital file. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or

two pixels, results in a different hash value. Consequently, an unknown image can be determined to be identical to an original file if it has the same hash value as the original. The hash value is, in essence, the unique fingerprint of that file, and when a match of the "fingerprint" occurs, the file also matches. Several different algorithms are commonly used to hash-identify files, including Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1).

8. Hash values are a very reliable method of authenticating files. It can be concluded with an extremely high degree of certainty that two files sharing the same hash value also share identical content. Based on my training and experience, as well as others in this field, I know it is more likely that two humans would share the same biological DNA than for two files to share the same hash value. If even one bit (the smallest measure of data in a file) of a file is changed, the entire hash value of that file changes completely. As an example, that demonstrates the uniqueness of a SHA-1 hash, the likelihood of two files having the same SHA-1 hash value is 2^{128} or:1 in 340,000,000,000,000,000,000,000,000,000,000,000,000 chance. In an August 6, 2020, article in Live Science, Professor Simona Francese, Ph. D., a forensic scientist and fingerprint expert from Sheffield Hallam University in the United Kingdom, estimated the likelihood of two humans having the same fingerprint is estimated to be one in 64,000,000,000.

9. For two different files to have the same hash value is called a *collision.* I know from experience that there have been no documented incidents of a collision involving SHA-1 hash values "in the wild" since its creation in 1995. I am, however, aware of a reported collision involving two files sharing the same SHA-1 value in a lab setting. This was done purposely by engineers at Google in 2017 under controlled conditions for the sole purpose of creating this collision. Even with this knowledge in mind, I am confident that the possibility of a suspected CSAM file reported in a CyberTip having the same hash value as an unrelated, non-criminal file is extremely unlikely. I believe hash value comparison is a highly reliable method of determining if two files are

the same or different, and that a confirmed hash match between two files is a forensic finding on a par with a DNA match or a fingerprint match.

10. ISPs typically maintain a database of hash values of files that they have determined to meet the federal definition of depictions of minors engaged in sexually explicit conduct found in 18 U.S.C. § 2256. The ISPs typically do not maintain the actual suspect files themselves; once a file is determined to contain suspected depictions of minors engaged in sexually explicit conduct, the file is deleted from their system.

11. The ISPs can then use Image Detection and Filtering Process ("IDFP"), Photo DNA (pDNA), or a similar technology which compares the hash values of files embedded in or attached to transmitted files against their database containing what is essentially a catalog of hash values of files that have previously been identified as containing suspected depictions of minors engaged in sexually explicit conduct.

12. When the ISP detects a file passing through its network that has the same hash value as an image or video file of suspected depictions of minors engaged in sexually explicit conduct contained in the database through a variety of methods, the ISP reports that fact to National Center for Missing and Exploited Children (NCMEC) via the latter's CyberTipline. By statute, an ESP or ISP has a duty to report to NCMEC any apparent depictions of minors engaged in sexually explicit conduct it discovers "as soon as reasonably possible." 18 U.S.C. § 2258A(a)(1). The CyberTipline report transmits the intercepted file to NCMEC. Often that occurs without an ISP employee opening or viewing the file because the files hash value, or "fingerprint," has already been associated to a file of suspected depictions of minors engaged in sexually explicit conduct. The ISP's decision to report a file to NCMEC is made solely on the basis of the match of the unique hash value of the suspected depictions of minors engaged in sexually explicit conduct to the identical hash value in the suspect transmission.

13. Most Internet Service Providers keep subscriber records relating to the IP address they assign, and that information is available to investigators. Typically, an

investigator has to submit legal process (e.g. subpoena or search warrant) requesting the subscriber information relating to a particular IP address at a specific date and time.

14. A variety of publicly available websites provide a public query/response protocol that is widely used for querying databases in order to determine the registrant or assignee of internet resources, such as a domain name or an IP address block. These include WHOIS, MaxMind, arin.net, and other common search tools.

15. The act of "downloading" is commonly described in computer networks as a means to receive data to a local system from a remote system, or to initiate such a data transfer. Examples of a remote system from which a download might be performed include a webserver, FTP server, email server, or other similar systems. A download can mean either any file that is offered for downloading or that has been downloaded, or the process of receiving such a file. The inverse operation, "uploading," refers to the sending of data from a local system to a remote system such as a server or another client with the intent that the remote system should store a copy of the data being transferred, or the initiation of such a process.

16. The National Center for Missing and Exploited Children (NCMEC) is a private, non-profit organization established in 1984 by the United States Congress. Primarily funded by the Justice Department, the NCMEC acts as an information clearinghouse and resource for parents, children, law enforcement agencies, schools, and communities to assist in locating missing children and to raise public awareness about ways to prevent child abduction, child sexual abuse and depictions of minors engaged in sexually explicit conduct.

17. The Center provides information to help locate children reported missing (by parental abduction, child abduction, or running away from home) and to assist physically and sexually abused children. In this resource capacity, the NCMEC distributes photographs of missing children and accepts tips and information from the public. It also coordinates these activities with numerous state and federal law enforcement agencies. The CyberTipline offers a means of reporting incidents of child

sexual exploitation including the possession, manufacture, and/or distribution of depictions of minors engaged in sexually explicit conduct; online enticement; child prostitution; child sex tourism; extra familial child sexual molestation; unsolicited obscene material sent to a child; and misleading domain names, words, or digital images.

18. Any incidents reported to the CyberTipline online or by telephone go through this three-step process: CyberTipline operators review and prioritize each lead; NCMEC's Exploited Children Division analyzes tips and conducts additional research; The information is accessible to the FBI, ICE, and the USPIS via a secure Web connection. Information is also forwarded to the ICACs and pertinent international, state, and local authorities and, when appropriate, to the ESP.

19. Files that obtain apparent or suspected child pornography content is categorized by NCMEC as A1, A2, B1, or B2. Content that is categorized as A involves a prepubescent minor and B categorization involves a pubescent minor. Content that is categorized as a rank of 1 involves a "sex act" and rank of 2 involves a "lascivious exhibition". A sex act is considered any imagery depicting sexual intercourse (including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction of the above that lacks serious literary, artistic, political, or scientific value. A lascivious exhibition is considered Any imagery depicting the lascivious exhibition of the anus, genitals, or pubic area of any person, where a minor is engaging in the lascivious exhibition or being used in connection with sexually explicit conduct, which may include but is not limited to imagery where the focal point is on the child's anus, genitals, or pubic area and where the depiction is intended or designed to elicit a sexual response in the viewer.

SUMMARY OF PROBABLE CAUSE

20. This case involves the investigation into allegations that three minor females, SYERA BILL (hereinafter referred to as S.B.), ARIEL FELICIANO (hereinafter referred to as A.F.), and ISABELLE CHEVAL (hereinafter referred to as I.C.) (referred to collectively as "MINOR VICTIMS)" are victims to child sexual exploitation or child sex trafficking.[1] These females have a high volume of runaway reports and law enforcement contacts with adult men from Guatemala and Mexico, including describing themselves to others as being in dating or sexually intimate relationships with these adult men. As set forth below, two of the MINOR VICTIMS have made statements to law enforcement that various adult males have picked up and driven the females to and from houses, bought them food or clothing, or provided them with marijuana and alcohol. They have further advised law enforcement that the MINOR VICTIMS met these men online and exchanged communications via Instagram or Facebook Messenger, Snapchat, or text messages. Approximately five of these men of these adult men were subsequently charged with child molestation and or rape charges of these juvenile females. At least ten additional men are under investigation for similar charges by the FBI and HSI.

21. In January 2025, Lummi Nation Police Department (LNPD) recovered A.F. and I.C., who had been reported as runaways. LNPD seized their phones and subsequently obtained search warrants related to the joint investigation with FBI and HSI of the sexual exploitation of the MINOR VICTIMS. These search warrants were obtained to identify evidence related to the alleged sexual exploitation and to identify the potential male subjects and communications exchange between I.C., A.F., and the adult men that are exploiting and/or trafficking them. These devices are still under review, but several social media accounts, phone numbers, and new adult males have been identified.

22. In January 2025, both I.C. and A.F. were forensically interviewed. Both confirmed names of adult men that law enforcement suspected of exploiting the MINOR

[1] Child sex trafficking is defined as a person under the age of 18 who the trafficker recruits, harbors, transports, provides, patronizes, solicits, or advertises for the purpose of the commercial sex act of the child. Furthermore, there is an intersection between drug-endangered-children with at least one parent battling a substance abuse and the risk of that child falling into the sex trade.

VICTIMS. I.C. and A.F. also provided new subject names were identified in the interviews, in addition to social media accounts and phone numbers used to communicate with these adult men.

23. In January 2025, the FBI contacted the National Center for Missing and Endangered Children (NCMEC) for any CyberTips related to the phone numbers, emails, account usernames, or common IP addresses tied to the subjects identified in the investigation thus far. On February 4, 2025, NCMEC returned several CyberTips that were submitted by Google, Facebook, Instagram, Roblox, and Snapchat. These were submitted by the ESPs, who reported that account users had uploaded suspected child pornography to its servers or engaged in communications that indicated enticement of minors for sexual purposes. The SUBJECT CYBERTIPS listed herein were submitted to NCMEC by Electronic Service Providers (ESPs) that did not view some or all of the SUBJECT FILES. I am seeking authority to open and examine them. The SUBJECT CYBERTIPS are listed in detail in Attachment A.

CONCLUSION

24. Based on the foregoing, I believe there is probable cause to conclude that evidence, fruits, and instrumentalities of violations of the TARGET OFFENSES, are located within the SUBJECT FILE as more fully described in Attachment A to this Affidavit. I therefore request that the Court issue a warrant authorizing a search of the SUBJECT FILE for the items more fully described in Attachment B and the seizure of any such items found therein.

Natalie Leavitt, Affiant
Special Agent
Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on 12th day of March 2025.

PAULA L. MCCANDLIS
United States Magistrate Judge

ATTACHMENT A

Description of Property to be Searched

The following SUBJECT FILES associated with the SUBJECT CYBERTIPS, which are stored on an encrypted thumb drive currently located at the FBI office in Bellingham, Washington.

CYBERTIP Number: 133426894

- Associated with: IP Address 216.243.2.254
- ESP: Facebook
- SUBJECT FILE Name: bZmdXIol7RJo7vcJ10000000_4980617235398308_4515015360492102484_n.mp4
- SUBJECT FILE Type: B1

CYBERTIP Number: 187960570

- Associated with: IP Address 168.212.80.1
- ESP: Snapchat
- SUBJECT FILE Names:
  - talan.bungard-None-e43ee7a5-ab77-5ca8-be61-d22a5d5235a3~2227- 5f0d0bce99-content.jpg
  - talan.bungard-None-e43ee7a5-ab77-5ca8-be61-d22a5d5235a3~2238- f162da0b54-content.jpg
  - talan.bungard-None-AD7A0531-1C3F-4CF6-9492-AAFC403A62DD-4512511459-content.jpg
- SUBJECT FILE Types: B2

CYBERTIP Number: 182657806

- Associated with: IP Address 168.212.80.1
- ESP: Instagram

- SUBJECT FILE Name: kHdi3N8UsA7Dpnln411201837_338749462237448_2227901945770862706_n.mp4
- SUBJECT FILE Type: B2

CYBERTIP Number: 186170387

- Associated with: IP Address 4.37.69.186
- ESP: Google
- SUBJECT FILE Names:
  - PVK_5116.jpg
  - PVK_5886 (3).jpg
- SUBJECT FILE Types: Not specified

CYBERTIP Number: 183500836

- Associated with: IP Address 4.37.69.186
- ESP: Instagram
- SUBJECT FILE Name: z1RezETQgyRcK15B414981859_24346419101668041_8734993716765846851_n.mp4
- SUBJECT FILE Type: B1

CYBERTIP Number: 204173525

- Associated with: username sin_mied00
- ESP: Instagram
- SUBJECT FILE Name: OKF9zj5UNVO9V7Rt462577400_2030519530709476_836042072494273043_n.jpg
- SUBJECT FILE Type: B1

CYBERTIP Number: 131334754

- Associated with: username jarvidylanr
- ESP: Facebook

- SUBJECT FILE Name: CC6InoOZrrGI2syO288244391_5247343785358433_4475858483811337 00_n.mp4
- SUBJECT FILE Type: Not specified

CYBERTIP Number: 11885149

- Associated with: username bellako_13
- ESP: Facebook
- SUBJECT FILE Names:
  - root-request-tempfiles7dnhaa660fgo0o4k13285671_624825027684548_1765048 393_n .jpg
  - root-request-tempfilesac7vlsaw1nsogggk13285671_624825027684548_1765048 393_n .jpg
- SUBJECT FILE Types: Not specified

CYBERTIP Number: 11884993

- Associated with: username bellako_13
- ESP: Facebook
- SUBJECT FILE Name: root-request-tempfilesdtmp0n18lds0c0kw13282063_1750882848459101_2117239048_ n.jpg
- SUBJECT FILE Type: Not specified

CYBERTIP Number: 72033948

- Associated with: everildo.mendoza.7
- ESP: Facebook
- SUBJECT FILE Name: 53ply2dz2rggow8095725654_2742387202550209_497172242117384061 8_n.mp4

- SUBJECT FILE Type: Not specified

CYBERTIP Number: 64996692

- Associated with: everildo.mendoza.7
- ESP: Facebook
- SUBJECT FILE Name: 20rr7g5r2r5wk4sg86802617_2905973956131291_6258471936714425512_n.mp4
- SUBJECT FILE Type: Not specified

CYBERTIP Number: 68660570

- Associated with: danieljuniorsantos127
- ESP: Facebook
- SUBJECT FILE Name: n99o5xwj828800cs92508571_599521230641971_4501033466015514624_o.jpg
- SUBJECT FILE Type: Not specified

ATTACHMENT B

ITEMS TO BE SEIZED

All information that constitutes evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found in the SUBJECT FILE:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct;

2. Information about the SUBJECT FILES related to the timing or circumstances of their creation and transmission; in any format or media;

3. Information concerning the identify of any individuals depicted in the SUBJECT FILES; and

4. Information or data that, including direct messages, postings, photos, or other account content that identifies the user(s) of the accounts associated with the SUBJECT FILES.